



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/996,671	11/30/2001	Donald R. Horne	13608ROUS02U	4165

626 7590 04/07/2005
NORTEL NETWORKS LIMITED
P. O. BOX 3511, STATION C
OTTAWA, ON K1Y 4H7
CANADA

EXAMINER

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 04/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/996,671	Applicant(s) HORNE, DONALD R.	
	Examiner Matthew T Henning	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 November 2001.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☒ Claim(s) 1,4-20,23 and 24 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 November 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2131

This action is in response to the communication filed on 11/30/2001.

DETAILED ACTION

1. Claims 1-24 have been examined.

Title

2. The title of the invention is acceptable.

Priority

3. The application has been filed under Title 35 U.S.C §119, claiming priority to Canada Application Number 2,327,211, filed 12/01/2000.

4. The effective filing date for the subject matter defined in the pending claims in this application is 12/01/2000.

Drawings

5. The drawings filed on 2/14/2002 are acceptable for examination proceedings.

Specification

6. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

7. The abstract of the disclosure is objected to because

Line 2: The phrase "is provided" can be implied and therefore must be removed.

Lines 1, 5, 8, and 14 contain legal phraseology (comprising), which must be removed.

Art Unit: 2131

The abstract is objected to for containing multiple paragraphs.

Correction is required. See MPEP § 608.01(b).

Claim Objections

8. Claims 4-13, 15-17, and 19-20 are objected to for failing to comply with the standard claim numbering as set forth in 37 CFR 1.75(c).

9. The applicant is reminded that a series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

10. Claims 1, 4-6, 7, 9-14, 18-20, and 23-24 are objected to because of the following informalities:

Claims 1, 4, 10-12, 14, 18-19, and 23-24 improperly use the word "archival" as a verb, where the word is actually an adjective, and should be used as such.

Claims 5-6 and 9 are objected to by virtue of their dependency to claim 4.

Claim 7 recites the limitation "wherein the data and system unit wherein" which does not make sense.

Claim 12 recites "(SM)" in line 3, which should read "(SM)".

Claim 13 line 4 should end with a ".".

Claim 13 Line 9 recites "logs form online to" which should read "logs from online to".

Appropriate correction is required.

Claim 17 Line 7 should recite "intrusion detection system".

Claim 18 Line 2 should end with a ' '.

Claim 20 recites the limitation "via a a data".

Claims 23 and 24 recite "for a data network security," which is incomplete.

Claim Rejections - 35 USC § 112

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 5, 10-13, 17, and 21-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

13. Claim 5 recites the limitation "the storage unit" in lines 5-6. There is insufficient antecedent basis for this limitation in the claim.

14. Claims 10-13 recite the limitation "SD logfiles" wherein "SD" is not defined in the claims. It is unclear whether this "SD" limitation is meant to restrict the type of logfiles in the claims to a particular type of logfile, and if so, what type of logfile that is. The ordinary person skilled in the art would therefore be unable to determine the scope of these claims. Therefore, claims 10-13 are rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

15. Claim 12 recites the limitation "individual LC" wherein "LC" is not defined in the claims. It is unclear what the limitation "LC" is referring to, and therefore the ordinary person skilled in the art would be unable to determine the scope of the claim. Therefore, claim 12 is

Art Unit: 2131

rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

16. Claim 13 recites the limitation "the SM log archival tables" in lines 12-13. There is insufficient antecedent basis for this limitation in the claim.

17. The term "easily" in claim 17 line 6 is a relative term which renders the claim indefinite. The term "easily" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. One of ordinary skill in the art would be unable to determine what makes interfaces easily protected via a firewall and intrusion detection system and what makes them not easily protected. Therefore, the ordinary person skilled in the art would be unable to determine the scope of the claim. For purposes of searching prior art, the examiner will assume the limitation should have read "whereby the interfaces are protected via a firewall and intrusion detection system."

18. Claim 21 Lines 9-10 recite the limitation "the SM log archival tables". There is insufficient antecedent basis for this limitation in the claim.

19. Claim 22 is rejected by virtue of its dependency to claim 21.

Claim Rejections - 35 USC § 102

20. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international

Art Unit: 2131

application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

21. Claims 1-5, 7, 9-16, and 18-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Proctor (US Patent Number 6,530,024).

22. Regarding claim 1, Proctor disclosed a security device log and reporting system for a data network (See Proctor Fig. 14), comprising: a Log Collection unit, for collecting log files from security devices (See Proctor Col. 15 Line 65 – Col. 16 Line 4), a Data Analysis and Log Archival unit for analysis and archival of log files (See Proctor Col. 16 Lines 5-26), and a Data and System Access Unit providing a user interface with the Data Analysis and Log Archival Unit (See Proctor Col. 16 Lines 54-58 and Fig. 14 Element 1454).

23. Regarding claim 2, Proctor disclosed that the Log Collection unit comprises a Log Manager for managing log collection from a plurality of security devices (See Proctor Col. 15 Line 65 – Col 16 Line 18).

24. Regarding claim 3, Proctor disclosed that the Log Collection Unit comprises a plurality of log collectors and a log collection manager for managing log collection from a plurality of log collectors (See Proctor Col. 15 Line 65 – Col 16 Line 18).

25. Regarding claim 4, Proctor disclosed a data network security management system for security device log archival and reporting comprising: a log collection unit comprising a plurality of log collectors, each for collecting log files from a plurality of security device nodes and a log manager for collecting log files from the plurality of log collectors (See Proctor Col. 15 Line 65 – Col 16 Line 18); a data analysis and log archival unit for archival and automated analysis of

Art Unit: 2131

log files transferred from the log manager (See Proctor Col. 16 Lines 5-26), and a data and system access unit providing a user interface to the Data Analysis and Log Archival Unit (See Proctor Col. 16 Lines 54-58 and Fig. 14 Element 1454).

26. Regarding claim 5, Proctor disclosed that the log collection unit provides output to a storage manager and a Data Analysis manager, connected to a Data Analysis Store, of the Data Analysis and Log Archival unit, which also comprises a Archival unit associated with the Storage unit (See Proctor Col. 16 Line 5 – 63).

27. Regarding claim 7, Proctor disclosed an interface for the system administrator and generating log analysis summaries, and trend analysis from the monitoring system (See Proctor Figs. 4-8, Col. 11 Paragraph 6- Col. 12 Paragraph 3 and Col. 16 Paragraph 7). Proctor further disclosed the interface providing for system configuration (See Proctor Fig. 4) and for controlled operational access (See Proctor Fig. 7).

28. Regarding claim 9, Proctor disclosed that the log collector receives logfiles from security devices comprising one or more device types comprising: Firewalls, CES, SPAM, FTP Drop Box and Anti-virus (See Proctor Col. 15 Line 65- Col. 16 Line 4 and Fig. 8 wherein the a log of antivirus activity was kept for each target).

29. Regarding claim 10, Proctor disclosed that the Log Manager LM interfaces with a Data Analysis Manager (DAM) and a Storage Manager (SM) (See Proctor Fig. 14) and the LM comprises: means for collecting logfiles from security devices (See Proctor Col. 15 Line 65 – Col. 16 Line 4), means for pushing cached SD logfiles to a Storage manager for archival (See Proctor Col. 16 Lines 5-18), and means for providing log archival status updates to a Data Analysis Manager (DAM) (See Proctor Col. 16 Lines 19-26).

Art Unit: 2131

30. Regarding claim 11, Proctor disclosed A Log Manager for a data network security management system, wherein the Log Manager LM interfaces with a Data Analysis Manager (DAM) and a Storage Manager (SM) (See Proctor Fig. 14) and the LM comprises: means for collecting logfiles from security devices (See Proctor Col. 15 Line 65 – Col. 16 Line 4), means for pushing cached SD logfiles to a Storage manager for archival (See Proctor Col. 16 Lines 5-18), and means for providing log archival status updates to a Data Analysis Manager (DAM) (See Proctor Col. 16 Lines 19-26).

31. Regarding claim 12, Proctor disclosed that the Log Collector Manager (LCM) interfaces with a Data Analysis Manager (DAM) and a Storage Manager (SM) (See Proctor Fig. 14) and the LCM comprises: means for receiving logfiles from the plurality of log collectors (See Proctor Col. 15 Line 65 – Col. 16 Line 4), means for obtaining a logging system configuration from the DAM (See Proctor Col. 16 Lines 43-51), means for propagating the configuration to individual LC associated with Security devices (See Proctor Col. 15 Line 65 – Col. 16 Line 4), means for providing notification to the LC to begin transfer of SD log files (See Proctor Col. 15 Line 65 – Col. 16 Line 4), and means for pushing cached SD log files to the Storage manager for archival (See Proctor Col. 16 Lines 5-18), and means for providing log archival status updates to the DAM (See Proctor Col. 16 Lines 19-26).

32. Regarding claim 13, Proctor disclosed that the Data Analysis and Log Archival unit comprises a Storage Manager (SM) and a Data Analysis Manager (DAM) (See Proctor Fig. 14) and the SM comprises means to receive security device logs from the Log Collector Manager (See Proctor Col. 15 Line 65 – Col. 16 Line 4), means for system archival (See Proctor Col. 16 Lines 5-18), means for management of online and offline log archivals and transition of logs

Art Unit: 2131

form online to offline status (See Proctor Col. 16 Lines 52-60), means to provide the Data Analysis Manager (DAM) with access to SD logs on request, and means to provide the DAM with access to the SM log Archival tables on request (See Proctor Col. 12 Paragraph 3).

33. Regarding claim 14, Proctor disclosed a security device log and reporting system wherein archival of log files is separated from analysis of logfiles (See Proctor Fig. 14 and related text).

34. Regarding claim 15, Proctor disclosed a security device log and reporting system comprising a Log Manager, the Log Manager having a distributed interface for receiving logfiles from a plurality of security devices, and is the interface to a Data Analysis and Archival unit of the system (See Proctor Fig. 14 and related text).

35. Regarding claim 16, Proctor disclosed that the Log manager comprises an intermediary caching system for log files received from the plurality of security devices (See Proctor Fig. 14 Element 1432).

36. Regarding claim 18, Proctor disclosed a method of managing security device log archival and reporting for a data network security, comprising collecting log files from a security device node at a log collector (See Proctor Col. 15 Paragraph 5), collecting log files from a plurality of log collectors at a log collection manager (See Proctor Col. 15 Line 65 – Col. 16 Line 4), transferring log files from the log collection manager to a data analysis and log archival unit for archival and analysis (See Proctor Col. 16 Lines 5-18).

37. Regarding claim 19, Proctor disclosed a method of managing security device log archival and reporting for a data network security, comprising collecting log files from a security device node at a log collector (See Proctor Col. 15 Paragraph 5), collecting log files from a plurality of log collectors at a log collection manager (See Proctor Col. 15 Line 65 – Col. 16 Line 4),

Art Unit: 2131

transferring log files from the log collection manager to a data analysis and log archival unit for archival and analysis (See Proctor Col. 16 Lines 5-18), logfile analysis being separated from log file archival (See Proctor Fig. 14).

38. Regarding claim 20, Proctor disclosed providing user access to the Data analysis and log archival unit via a data and system access unit (See Proctor Col. 16 Paragraph 7 and Col. 12 Paragraph 3).

39. Regarding claim 21, Proctor disclosed a Storage Manager for a security device log archival and reporting system comprising means for receiving security device logs from the log collector manager for system archival (See Proctor Col. 15 Line 65 – Col. 16 Line 4), means for management of online and offline log archival and transition of logs from online to offline status (See Proctor Col. 16 Paragraph 7), means for providing the DAM with access to security device logs on request, means for providing the DAM with access to the SM log archival tables on request (See Proctor Col. 12 Paragraph 3).

40. Regarding claim 22, Proctor disclosed means for differentiating types of log files (See Proctor Col. 15 Paragraph 5).

41. Regarding claim 23, Proctor disclosed a computer readable medium for implementing a method of managing security device log archival and reporting for a data network security , comprising collecting log files from a security device node at a log collector collecting log files from a plurality of log collectors at a log collection manager transferring log files from the log collection manager to a data analysis and log archival unit for archival and analysis (See the rejection of claim 18 above and further see Proctor Col. 17 Paragraph 2).

42. Regarding claim 24, see the rejection of claim 19 above.

Art Unit: 2131

Claim Rejections - 35 USC § 103

43. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

44. Claims 6 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor as applied to claims 1 and 4 above, and further in view of Landan (US Patent Number 6,449,739).

Proctor disclosed a user interface (See Proctor Figures 4-9), but failed to disclose the interface being web-based and authenticated, authorized and secure.

Landan teaches that monitoring interfaces should be web-based and should also be secured using authentication and authorization (See Landan Col. 12 Paragraph 4 and Col. 16 Lines 49-60).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Landan in the monitoring system of Proctor by having the user interface be a secured web-based interface. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide the flexibility of allowing the administrator to access the system from any computer connected to the Internet, instead of just the security console.

Art Unit: 2131

45. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor as applied to claim 14 above, and further in view of Holland, III et al. (US patent Number 6,851,061) hereinafter referred to as Holland.

Proctor disclosed an Data Analysis and Archival Unit (See Proctor Col. 16 Paragraph 2), a Log Collection Unit comprising a Log Manager (See Proctor Col. 15 Line 65 – Col. 16 Line 4), and Data and system Access Unit (See Proctor Col. 16 Paragraph 7), wherein Data Analysis and Archival Unit interfaces with only a Log Manager and a Data and System Access Units (See Proctor Fig. 14), but failed to disclose that interfaces are easily protected via a firewall and intrusion detection system. However, Proctor did disclose the targets being separated from the monitoring system by the Internet (See Proctor Col. 17 Line 53 – Col. 18 Line 2).

Holland teaches that firewalls prevent unauthorized access to an intranetwork, and that intrusion detection systems detect attempts or actual compromises of network or system security.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Holland in the monitoring system of Proctor by placing a firewall and an intrusion detection system at the interfaces of the networks. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against unauthorized access to the monitoring system.

Conclusion

46. Claims 1-24 have been rejected.

47. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.


Art Unit: 2131

- a. Boyd et al. (US Patent Number 6,317,787) disclosed a system for archiving and analyzing collected logs.
- b. Shah et al. (US Patent Number 6,678,835) disclosed a system for collecting logs as well as archiving them and analyzing them.
- c. Singer et al. (US Patent Number 6,789,115) disclosed a system for collecting server usage data, and analyzing the usage data.

48. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Matthew Henning
Assistant Examiner
Art Unit 2131
3/31/2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100